

CISA Dumps

Isaca CISA

<https://www.certleader.com/CISA-dumps.html>



NEW QUESTION 1

- (Topic 1)

Which of the following is a benefit of using callback devices?

- A. Provide an audit trail
- B. Can be used in a switchboard environment
- C. Permit unlimited user mobility
- D. Allow call forwarding

Answer: A

Explanation:

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

NEW QUESTION 2

- (Topic 1)

A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

- A. dials back to the user machine based on the user id and password using a telephone number from its databas
- B. dials back to the user machine based on the user id and password using a telephone number provided by the user during this connectio
- C. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its databas
- D. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's databas

Answer: A

Explanation:

A call-back system in a net centric environment would mean that a user with an id and password calls a remote server through a dial-up line first, and then the server disconnects and dials back to the user machine based on the user id and password using a telephone number from its database. Although the server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

NEW QUESTION 3

- (Topic 1)

A database administrator is responsible for:

- A. defining data ownershi
- B. establishing operational standards for the data dictionar
- C. creating the logical and physical databas
- D. establishing ground rules for ensuring data integrity and securit

Answer: C

Explanation:

A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

NEW QUESTION 4

- (Topic 1)

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

- A. digest signatur
- B. electronic signatur
- C. digital signatur
- D. hash signatur

Answer: C

Explanation:

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

NEW QUESTION 5

- (Topic 1)

Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

- A. Gateway
- B. Protocol converter
- C. Front-end communication processor

D. Concentrator/multiplexor

Answer: A

Explanation:

A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks.

NEW QUESTION 6

- (Topic 1)

A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

- A. duplicate chec
- B. table looku
- C. validity chec
- D. parity chec

Answer: D

Explanation:

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

NEW QUESTION 7

- (Topic 1)

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

- A. Paper test
- B. Post test
- C. Preparedness test
- D. Walk-through

Answer: C

Explanation:

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments.

NEW QUESTION 8

- (Topic 1)

The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

- A. Relocate the shut off switc
- B. Install protective cover
- C. Escort visitor
- D. Log environmental failure

Answer: B

Explanation:

A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation.

NEW QUESTION 9

- (Topic 1)

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- A. registration authority (RA).
- B. issuing certification authority (CA).
- C. subject C
- D. policy management authorit

Answer: A

Explanation:

A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

NEW QUESTION 10

- (Topic 1)

What is the primary objective of a control self-assessment (CSA) program?

- A. Enhancement of the audit responsibility
- B. Elimination of the audit responsibility
- C. Replacement of the audit responsibility
- D. Integrity of the audit responsibility

Answer: A

Explanation:

Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

NEW QUESTION 10

- (Topic 1)

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- A. The same value
- B. Greater value
- C. Lesser value
- D. Prior audit reports are not relevant

Answer: C

Explanation:

Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

NEW QUESTION 11

- (Topic 1)

What is the PRIMARY purpose of audit trails?

- A. To document auditing efforts
- B. To correct data integrity errors
- C. To establish accountability and responsibility for processed transactions
- D. To prevent unauthorized access to data

Answer: C

Explanation:

The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

NEW QUESTION 15

- (Topic 1)

The use of statistical sampling procedures helps minimize:

- A. Detection risk
- B. Business risk
- C. Controls risk
- D. Compliance risk

Answer: A

Explanation:

The use of statistical sampling procedures helps minimize detection risk.

NEW QUESTION 20

- (Topic 1)

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

- A. True
- B. False

Answer: A

Explanation:

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions.

NEW QUESTION 22

- (Topic 1)

Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

- A. True
- B. False

Answer: B

Explanation:

Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities.

NEW QUESTION 23

- (Topic 1)

If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

- A. IT cannot be implemented if senior management is not committed to strategic planning
- B. More likely
- C. Less likely
- D. Strategic planning does not affect the success of a company's implementation of IT

Answer: C

Explanation:

A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning.

NEW QUESTION 28

- (Topic 1)

Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

- A. Lack of employee awareness of a company's information security policy
- B. Failure to comply with a company's information security policy
- C. A momentary lapse of reason
- D. Lack of security policy enforcement procedures

Answer: A

Explanation:

Lack of employee awareness of a company's information security policy could lead to an unintentional loss of confidentiality.

NEW QUESTION 33

- (Topic 1)

What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

- A. A star network topology
- B. A mesh network topology with packet forwarding enabled at each host
- C. A bus network topology
- D. A ring network topology

Answer: B

Explanation:

A mesh network topology provides a point-to-point link between every network host. If each host is configured to route and forward communication, this topology provides the greatest redundancy of routes and the greatest network fault tolerance.

NEW QUESTION 35

- (Topic 1)

An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

- A. Evidence collected through personal observation
- B. Evidence collected through systems logs provided by the organization's security administration
- C. Evidence collected through surveys collected from internal staff
- D. Evidence collected through transaction reports provided by the organization's IT administration

Answer: A

Explanation:

An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

NEW QUESTION 38

- (Topic 1)

What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

- A. Nonconnection-oriented protocols
- B. Connection-oriented protocols
- C. Session-oriented protocols
- D. Nonsession-oriented protocols

Answer: B

Explanation:

The transport layer of the TCP/IP protocol suite provides for connection-oriented protocols to ensure reliable communication.

NEW QUESTION 39

- (Topic 1)

Why does the IS auditor often review the system logs?

- A. To get evidence of password spoofing
- B. To get evidence of data copy activities
- C. To determine the existence of unauthorized access to data by a user or program
- D. To get evidence of password sharing

Answer: C

Explanation:

When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs.

NEW QUESTION 42

- (Topic 1)

What is essential for the IS auditor to obtain a clear understanding of network management?

- A. Security administrator access to systems
- B. Systems logs of all hosts providing application services
- C. A graphical map of the network topology
- D. Administrator access to systems

Answer: C

Explanation:

A graphical interface to the map of the network topology is essential for the IS auditor to obtain a clear understanding of network management.

NEW QUESTION 43

- (Topic 1)

How is risk affected if users have direct access to a database at the system level?

- A. Risk of unauthorized access increases, but risk of untraceable changes to the database decrease
- B. Risk of unauthorized and untraceable changes to the database increase
- C. Risk of unauthorized access decreases, but risk of untraceable changes to the database increase
- D. Risk of unauthorized and untraceable changes to the database decrease

Answer: B

Explanation:

If users have direct access to a database at the system level, risk of unauthorized and untraceable changes to the database increases.

NEW QUESTION 48

- (Topic 1)

What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management? Choose the BEST answer.

- A. The software can dynamically readjust network traffic capabilities based upon current usage
- B. The software produces nice reports that really impress management
- C. It allows users to properly allocate resources and ensure continuous efficiency of operation
- D. It allows management to properly allocate resources and ensure continuous efficiency of operation

Answer: D

Explanation:

Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations.

NEW QUESTION 51

- (Topic 1)

How does the SSL network protocol provide confidentiality?

- A. Through symmetric encryption such as RSA
- B. Through asymmetric encryption such as Data Encryption Standard, or DES
- C. Through asymmetric encryption such as Advanced Encryption Standard, or AES
- D. Through symmetric encryption such as Data Encryption Standard, or DES

Answer: D

Explanation:

The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption Standard, or DES.

NEW QUESTION 52

- (Topic 1)

Which of the following is a good control for protecting confidential data residing on a PC?

- A. Personal firewall
- B. File encapsulation
- C. File encryption
- D. Host-based intrusion detection

Answer: C

Explanation:

File encryption is a good control for protecting confidential data residing on a PC.

NEW QUESTION 57

- (Topic 1)

Which of the following is a guiding best practice for implementing logical access controls?

- A. Implementing the Biba Integrity Model
- B. Access is granted on a least-privilege basis, per the organization's data owners
- C. Implementing the Take-Grant access control model
- D. Classifying data according to the subject's requirements

Answer: B

Explanation:

Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

NEW QUESTION 59

- (Topic 1)

What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

- A. A combination of public-key cryptography and digital certificates and two-factor authentication
- B. A combination of public-key cryptography and two-factor authentication
- C. A combination of public-key cryptography and digital certificates
- D. A combination of digital certificates and two-factor authentication

Answer: C

Explanation:

PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

NEW QUESTION 60

- (Topic 1)

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.

- A. Employee security awareness training
- B. Administrator alerts
- C. Screensaver passwords
- D. Close supervision

Answer: C

Explanation:

Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off.

NEW QUESTION 61

- (Topic 1)

What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

- A. OSI Layer 2 switches with packet filtering enabled
- B. Virtual Private Networks
- C. Access Control Lists (ACL)
- D. Point-to-Point Tunneling Protocol

Answer: C

Explanation:

ISPs can use access control lists to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources.

NEW QUESTION 65

- (Topic 1)

Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

- A. Assigning user access privileges
- B. Developing organizational security policies
- C. Creating roles and responsibilities
- D. Classifying data

Answer: D

Explanation:

To properly implement data classification, establishing data ownership is an important first step.

NEW QUESTION 66

- (Topic 1)

Which of the following is MOST critical during the business impact assessment phase of business continuity planning?

- A. End-user involvement
- B. Senior management involvement
- C. Security administration involvement
- D. IS auditing involvement

Answer: A

Explanation:

End-user involvement is critical during the business impact assessment phase of business continuity planning.

NEW QUESTION 71

- (Topic 1)

Which of the following typically focuses on making alternative processes and resources available for transaction processing?

- A. Cold-site facilities
- B. Disaster recovery for networks
- C. Diverse processing
- D. Disaster recovery for systems

Answer: D

Explanation:

Disaster recovery for systems typically focuses on making alternative processes and resources available for transaction processing.

NEW QUESTION 74

- (Topic 1)

Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

- A. Cold site
- B. Alternate site
- C. Hot site
- D. Warm site

Answer: A

Explanation:

Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

NEW QUESTION 79

- (Topic 1)

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following? Choose the BEST answer.

- A. IT strategic plan
- B. Business continuity plan
- C. Business impact analysis
- D. Incident response plan

Answer: B

Explanation:

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

NEW QUESTION 83

- (Topic 1)

What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

- A. Configuring software
- B. Planning security
- C. Determining time and resource requirements
- D. Configuring hardware

Answer: C

Explanation:

Determining time and resource requirements for an application-development project is often the most difficult part of initial efforts in application development.

NEW QUESTION 87

- (Topic 1)

What is a primary high-level goal for an auditor who is reviewing a system development project?

- A. To ensure that programming and processing environments are segregated

- B. To ensure that proper approval for the project has been obtained
- C. To ensure that business objectives are achieved
- D. To ensure that projects are monitored and administrated effectively

Answer: C

Explanation:

A primary high-level goal for an auditor who is reviewing a systems-development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

NEW QUESTION 90

- (Topic 1)

If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

- A. Documentation development
- B. Comprehensive integration testing
- C. Full unit testing
- D. Full regression testing

Answer: B

Explanation:

If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further comprehensive integration testing.

NEW QUESTION 95

- (Topic 1)

Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

- A. Function Point Analysis (FPA)
- B. GANTT
- C. Rapid Application Development (RAD)
- D. PERT

Answer: D

Explanation:

PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

NEW QUESTION 97

- (Topic 1)

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

- A. True
- B. False

Answer: A

Explanation:

Fourth-generation languages(4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

NEW QUESTION 101

- (Topic 1)

Run-to-run totals can verify data through which stage(s) of application processing?

- A. Initial
- B. Various
- C. Final
- D. Output

Answer: B

Explanation:

Run-to-run totals can verify data through various stages of application processing.

NEW QUESTION 103

- (Topic 1)

Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

- A. True
- B. False

Answer: A

Explanation:

Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

NEW QUESTION 104

- (Topic 1)

Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

- A. Redundancy check
- B. Completeness check
- C. Accuracy check
- D. Parity check

Answer: A

Explanation:

A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of data.

NEW QUESTION 106

- (Topic 1)

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

- A. True
- B. False

Answer: B

Explanation:

An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

NEW QUESTION 111

- (Topic 1)

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

- A. Implementor
- B. Facilitator
- C. Developer
- D. Sponsor

Answer: B

Explanation:

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

NEW QUESTION 113

- (Topic 1)

Which of the following is of greatest concern to the IS auditor?

- A. Failure to report a successful attack on the network
- B. Failure to prevent a successful attack on the network
- C. Failure to recover from a successful attack on the network
- D. Failure to detect a successful attack on the network

Answer: A

Explanation:

Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

NEW QUESTION 114

- (Topic 1)

An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

- A. True
- B. False

Answer: A

Explanation:

It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

NEW QUESTION 116

- (Topic 1)

Ensuring that security and control policies support business and IT objectives is a primary objective of:

- A. An IT security policies audit
- B. A processing audit
- C. A software audit
- D. A vulnerability assessment

Answer: A

Explanation:

Ensuring that security and control policies support business and IT objectives is a primary objective of an IT security policies audit.

NEW QUESTION 121

- (Topic 1)

When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

- A. Ownership of the programs and files
- B. A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster
- C. A statement of due care
- D. Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

Answer: D

Explanation:

When auditing third-party service providers, an auditor should be concerned with ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster.

NEW QUESTION 126

- (Topic 1)

When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

- A. True
- B. False

Answer: B

Explanation:

When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

NEW QUESTION 129

- (Topic 1)

Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

- A. True
- B. False

Answer: A

Explanation:

Allowing application programmers to directly patch or change code in production programs increases risk of fraud.

NEW QUESTION 132

- (Topic 1)

Who should be responsible for network security operations?

- A. Business unit managers
- B. Security administrators
- C. Network administrators
- D. IS auditors

Answer: B

Explanation:

Security administrators are usually responsible for network security operations.

NEW QUESTION 137

- (Topic 1)

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

- A. True
- B. False

Answer: A

Explanation:

Proper segregation of duties does not prohibit a quality-control administrator from also being responsible for change control and problem management.

NEW QUESTION 140

- (Topic 1)

What can be implemented to provide the highest level of protection from external attack?

- A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- B. Configuring the firewall as a screened host behind a router
- C. Configuring the firewall as the protecting bastion host
- D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Answer: A

Explanation:

Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

NEW QUESTION 142

- (Topic 1)

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

- A. The data should be deleted and overwritten with binary 0
- B. The data should be demagnetize
- C. The data should be low-level formatte
- D. The data should be delete

Answer: B

Explanation:

To properly protect against unauthorized disclosure of sensitive data, hard disks should be demagnetized before disposal or release.

NEW QUESTION 146

- (Topic 1)

Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

- A. True
- B. False

Answer: A

Explanation:

Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

NEW QUESTION 151

- (Topic 1)

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

- A. Modems convert analog transmissions to digital, and digital transmission to analo
- B. Modems encapsulate analog transmissions within digital, and digital transmissions within analo
- C. Modems convert digital transmissions to analog, and analog transmissions to digita
- D. Modems encapsulate digital transmissions within analog, and analog transmissions within digita

Answer: A

Explanation:

Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

NEW QUESTION 152

- (Topic 1)

What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

- A. A first-generation packet-filtering firewall
- B. A circuit-level gateway
- C. An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
- D. An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Answer: C

Explanation:

An application-layer gateway, or proxy firewall, and stateful-inspection firewalls provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

NEW QUESTION 154

- (Topic 1)

Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

- A. Automated electronic journaling and parallel processing
- B. Data mirroring and parallel processing
- C. Data mirroring
- D. Parallel processing

Answer: B

Explanation:

Data mirroring and parallel processing are both used to provide near-immediate recoverability for time-sensitive systems and transaction processing.

NEW QUESTION 157

- (Topic 1)

What is an effective control for granting temporary access to vendors and external support personnel? Choose the BEST answer.

- A. Creating user accounts that automatically expire by a predetermined date
- B. Creating permanent guest accounts for temporary use
- C. Creating user accounts that restrict logon access to certain hours of the day
- D. Creating a single shared vendor administrator account on the basis of least-privileged access

Answer: A

Explanation:

Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

NEW QUESTION 162

- (Topic 1)

Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack? Choose the BEST answer.

- A. Inbound traffic filtering
- B. Using access control lists (ACLs) to restrict inbound connection attempts
- C. Outbound traffic filtering
- D. Recentralizing distributed systems

Answer: C

Explanation:

Outbound traffic filtering can help prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack.

NEW QUESTION 166

- (Topic 1)

What is/are used to measure and ensure proper network capacity management and availability of services? Choose the BEST answer.

- A. Network performance-monitoring tools
- B. Network component redundancy
- C. Syslog reporting
- D. IT strategic planning

Answer: A

Explanation:

Network performance-monitoring tools are used to measure and ensure proper network capacity management and availability of services.

NEW QUESTION 171

- (Topic 1)

What is a callback system?

- A. It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fail
- B. It is a remote-access system whereby the user's application automatically redials the remoteaccess server if the initial connection attempt fail
- C. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration databas
- D. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of tim

Answer: C

Explanation:

A callback system is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

NEW QUESTION 174

- (Topic 1)

What determines the strength of a secret key within a symmetric key cryptosystem?

- A. A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key

- B. A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
- C. A combination of key length and the complexity of the data-encryption algorithm that uses the key
- D. Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Answer: B

Explanation:

The strength of a secret key within a symmetric key cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

NEW QUESTION 178

- (Topic 1)

What is often assured through table link verification and reference checks?

- A. Database integrity
- B. Database synchronization
- C. Database normalcy
- D. Database accuracy

Answer: A

Explanation:

Database integrity is most often ensured through table link verification and reference checks.

NEW QUESTION 179

- (Topic 1)

When should systems administrators first assess the impact of applications or systems patches?

- A. Within five business days following installation
- B. Prior to installation
- C. No sooner than five business days following installation
- D. Immediately following installation

Answer: B

Explanation:

Systems administrators should always assess the impact of patches before installation.

NEW QUESTION 181

- (Topic 1)

Which of the following is of greatest concern when performing an IS audit?

- A. Users' ability to directly modify the database
- B. Users' ability to submit queries to the database
- C. Users' ability to indirectly modify the database
- D. Users' ability to directly view the database

Answer: A

Explanation:

A major IS audit concern is users' ability to directly modify the database.

NEW QUESTION 185

- (Topic 1)

If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

- A. True
- B. False

Answer: A

Explanation:

If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions.

NEW QUESTION 189

- (Topic 1)

An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

- A. True
- B. False

Answer: B

Explanation:

An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage.

NEW QUESTION 191

- (Topic 1)

Which of the following is the dominating objective of BCP and DRP?

- A. To protect human life
- B. To mitigate the risk and impact of a business interruption
- C. To eliminate the risk and impact of a business interruption
- D. To transfer the risk and impact of a business interruption

Answer: A

Explanation:

Although the primary business objective of BCP and DRP is to mitigate the risk and impact of a business interruption, the dominating objective remains the protection of human life.

NEW QUESTION 194

- (Topic 1)

Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following? Choose the BEST answer.

- A. Financial reporting
- B. Sales reporting
- C. Inventory reporting
- D. Transaction processing

Answer: D

Explanation:

Off-site data storage should be kept synchronized when preparing for the recovery of timesensitive data such as that resulting from transaction processing.

NEW QUESTION 196

- (Topic 1)

Why is a clause for requiring source code escrow in an application vendor agreement important?

- A. To segregate systems development and live environments
- B. To protect the organization from copyright disputes
- C. To ensure that sufficient code is available when needed
- D. To ensure that the source code remains available even if the application vendor goes out of business

Answer: D

Explanation:

A clause for requiring source code escrow in an application vendor agreement is important to ensure that the source code remains available even if the application vendor goes out of business.

NEW QUESTION 198

- (Topic 1)

What uses questionnaires to lead the user through a series of choices to reach a conclusion? Choose the BEST answer.

- A. Logic trees
- B. Decision trees
- C. Decision algorithms
- D. Logic algorithms

Answer: B

Explanation:

Decision trees use questionnaires to lead the user through a series of choices to reach a conclusion.

NEW QUESTION 199

- (Topic 1)

What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

- A. Assigning copyright to the organization
- B. Program back doors
- C. Source code escrow
- D. Internal programming expertise

Answer: C

Explanation:

Source code escrow protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business.

NEW QUESTION 204

- (Topic 1)

Who is ultimately responsible for providing requirement specifications to the software-development team?

- A. The project sponsor
- B. The project members
- C. The project leader
- D. The project steering committee

Answer: A

Explanation:

The project sponsor is ultimately responsible for providing requirement specifications to the software-development team.

NEW QUESTION 207

- (Topic 1)

What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

- A. Contrived data
- B. Independently created data
- C. Live data
- D. Data from previous tests

Answer: D

Explanation:

Regression testing should use data from previous tests to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors.

NEW QUESTION 209

- (Topic 1)

Which of the following processes are performed during the design phase of the systemsdevelopment life cycle (SDLC) model?

- A. Develop test plan
- B. Baseline procedures to prevent scope creep
- C. Define the need that requires resolution, and map to the major requirements of the solution
- D. Program and test the new system
- E. The tests verify and validate what has been developed

Answer: B

Explanation:

Procedures to prevent scope creep are baselined in the design phase of the systems-development life cycle (SDLC) model.

NEW QUESTION 210

- (Topic 1)

When should application controls be considered within the system-development process?

- A. After application unit testing
- B. After application module testing
- C. After applications systems testing
- D. As early as possible, even in the development of the project's functional specifications

Answer: D

Explanation:

Application controls should be considered as early as possible in the system-development process, even in the development of the project's functional specifications.

NEW QUESTION 215

- (Topic 1)

What is the most common reason for information systems to fail to meet the needs of users? Choose the BEST answer.

- A. Lack of funding
- B. Inadequate user participation during system requirements definition
- C. Inadequate senior management participation during system requirements definition
- D. Poor IT strategic planning

Answer: B

Explanation:

Inadequate user participation during system requirements definition is the most common reason for information systems to fail to meet the needs of users.

NEW QUESTION 218

- (Topic 1)

Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

- A. Failing to perform user acceptance testing
- B. Lack of user training for the new system
- C. Lack of software documentation and run manuals

D. Insufficient unit, module, and systems testing

Answer: A

Explanation:

Above almost all other concerns, failing to perform user acceptance testing often results in the greatest negative impact on the implementation of new application software.

NEW QUESTION 223

- (Topic 1)

Input/output controls should be implemented for which applications in an integrated systems environment?

- A. The receiving application
- B. The sending application
- C. Both the sending and receiving applications
- D. Output on the sending application and input on the receiving application

Answer: C

Explanation:

Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

NEW QUESTION 226

- (Topic 1)

Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following? Choose the BEST answer.

- A. Unsynchronized transactions
- B. Unauthorized transactions
- C. Inaccurate transactions
- D. Incomplete transactions

Answer: B

Explanation:

Authentication techniques for sending and receiving data between EDI systems are crucial to prevent unauthorized transactions.

NEW QUESTION 231

- (Topic 1)

After identifying potential security vulnerabilities, what should be the IS auditor's next step?

- A. To evaluate potential countermeasures and compensatory controls
- B. To implement effective countermeasures and compensatory controls
- C. To perform a business impact analysis of the threats that would exploit the vulnerabilities
- D. To immediately advise senior management of the findings

Answer: C

Explanation:

After identifying potential security vulnerabilities, the IS auditor's next step is to perform a business impact analysis of the threats that would exploit the vulnerabilities.

NEW QUESTION 236

- (Topic 1)

Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

- A. Exposures
- B. Threats
- C. Hazards
- D. Insufficient controls

Answer: B

Explanation:

Threats exploit vulnerabilities to cause loss or damage to the organization and its assets.

NEW QUESTION 239

- (Topic 1)

Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

- A. Deterrent integrity controls
- B. Detective integrity controls
- C. Corrective integrity controls
- D. Preventative integrity controls

Answer: D

Explanation:

Data edits are implemented before processing and are considered preventive integrity controls.

NEW QUESTION 241

- (Topic 2)

An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

- A. variable samplin
- B. substantive testin
- C. compliance testin
- D. stop-or-go samplin

Answer: C

Explanation:

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

NEW QUESTION 243

- (Topic 2)

The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

- A. Inherent
- B. Detection
- C. Control
- D. Business

Answer: B

Explanation:

Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks are not usually affected by an IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by an IS auditor.

NEW QUESTION 246

- (Topic 2)

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

- A. scheduling may be performed months in advanc
- B. budgets are more likely to be met by the IS audit staf
- C. staff will be exposed to a variety of technologie
- D. resources are allocated to the areas of highest concern

Answer: D

Explanation:

The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be prepared months in advance using various scheduling methods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year.

NEW QUESTION 247

- (Topic 2)

The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

- A. information assets are overprotecte
- B. a basic level of protection is applied regardless of asset valu
- C. appropriate levels of protection are applied to information asset
- D. an equal proportion of resources are devoted to protecting all information asset

Answer: C

Explanation:

Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or underprotected. The risk assessment approach will ensure an appropriate level of protection is applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

NEW QUESTION 249

- (Topic 2)

An organization's IS audit charter should specify the:

- A. short- and long-term plans for IS audit engagements

- B. objectives and scope of IS audit engagement
- C. detailed training plan for the IS audit staff
- D. role of the IS audit function

Answer: D

Explanation:

An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee. Short-term and long-term planning is the responsibility of audit management. The objectives and scope of each IS audit should be agreed to in an engagement letter. A training plan, based on the audit plan, should be developed by audit management.

NEW QUESTION 254

- (Topic 2)

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

- A. address audit objective
- B. collect sufficient evidence
- C. specify appropriate test
- D. minimize audit resource

Answer: A

Explanation:

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning. The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

NEW QUESTION 255

- (Topic 2)

An IS auditor evaluating logical access controls should FIRST:

- A. document the controls applied to the potential access paths to the system
- B. test controls over the access paths to determine if they are functioning
- C. evaluate the security environment in relation to written policies and practices
- D. obtain an understanding of the security risks to information processing

Answer: D

Explanation:

When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

NEW QUESTION 259

- (Topic 2)

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

- A. Issue an audit finding
- B. Seek an explanation from IS management
- C. Review the classifications of data held on the server
- D. Expand the sample of logs reviewed

Answer: D

Explanation:

Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.

NEW QUESTION 260

- (Topic 2)

In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

- A. CASE tools
- B. Embedded data collection tools
- C. Heuristic scanning tools
- D. Trend/variance detection tools

Answer: D

Explanation:

Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for prenumbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

NEW QUESTION 261

- (Topic 2)

An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

- A. matching control totals of the imported data to control totals of the original dat
- B. sorting the data to confirm whether the data are in the same order as the original dat
- C. reviewing the printout of the first 100 records of original data with the first 100 records of imported dat
- D. filtering data for different categories and matching them to the original dat

Answer: A

Explanation:

Matching control totals of the imported data with control totals of the original data is the next logical step, as this confirms the completeness of the imported data. It is not possible to confirm completeness by sorting the imported data, because the original data may not be in sorted order. Further, sorting does not provide control totals for verifying completeness. Reviewing a printout of 100 records of original data with 100 records of imported data is a process of physical verification and confirms the accuracy of only these records. Filtering data for different categories and matching them to original data would still require that control totals be developed to confirm the completeness of the data.

NEW QUESTION 264

CORRECT TEXT - (Topic 2)

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

- A. Test data
- B. Generalized audit software
- C. Integrated test facility
- D. Embedded audit module

Answer: B

NEW QUESTION 268

- (Topic 2)

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

- A. identify and assess the risk assessment process used by management
- B. identify information assets and the underlying system
- C. disclose the threats and impacts to management
- D. identify and evaluate the existing control

Answer: D

Explanation:

It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

NEW QUESTION 269

- (Topic 2)

Which of the following would normally be the MOST reliable evidence for an auditor?

- A. A confirmation letter received from a third party verifying an account balance
- B. Assurance from line management that an application is working as designed
- C. Trend data obtained from World Wide Web (Internet) sources
- D. Ratio analysts developed by the IS auditor from reports supplied by line management

Answer: A

Explanation:

Evidence obtained from independent third parties almost always is considered to be the most reliable. Choices B, C and D would not be considered as reliable.

NEW QUESTION 271

- (Topic 2)

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

- A. Discussion with management
- B. Review of the organization chart

- C. Observation and interviews
- D. Testing of user access rights

Answer: C

Explanation:

By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

NEW QUESTION 275

- (Topic 2)

Data flow diagrams are used by IS auditors to:

- A. order data hierarchically
- B. highlight high-level data definition
- C. graphically summarize data paths and storage
- D. portray step-by-step details of data generation

Answer: C

Explanation:

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

NEW QUESTION 278

- (Topic 2)

An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

- A. Availability of online network documentation
- B. Support of terminal access to remote hosts
- C. Handling file transfer between hosts and interuser communications
- D. Performance management, audit and control

Answer: A

Explanation:

Network operating system user features include online availability of network documentation. Other features would be user access to various resources of network hosts, user authorization to access particular resources, and the network and host computers used without special user actions or commands. Choices B, C and D are examples of network operating systems functions.

NEW QUESTION 282

- (Topic 2)

The BEST method of proving the accuracy of a system tax calculation is by:

- A. detailed visual review and analysis of the source code of the calculation programs
- B. recreating program logic using generalized audit software to calculate monthly total
- C. preparing simulated transactions for processing and comparing the results to predetermined result
- D. automatic flowcharting and analysis of the source code of the calculation program

Answer: C

Explanation:

Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

NEW QUESTION 286

- (Topic 2)

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- A. analysis
- B. evaluation
- C. preservation
- D. disclosure

Answer: C

Explanation:

Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the acceptance of the evidence in legal proceedings. Analysis, evaluation and disclosure are important

but not of primary concern in a forensic investigation.

NEW QUESTION 290

- (Topic 2)

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- A. understand the business proces
- B. comply with auditing standard
- C. identify control weaknes
- D. plan substantive testin

Answer: A

Explanation:

Understanding the business process is the first step an IS auditor needs to perform. Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

NEW QUESTION 291

- (Topic 2)

In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

- A. examine source program changes without information from IS persone
- B. detect a source program change made between acquiring a copy of the source and the comparison ru
- C. confirm that the control copy is the current version of the production progra
- D. ensure that all changes made in the current source copy are detecte

Answer: A

Explanation:

An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes. Choice B is incorrect, because the changes made since the acquisition of the copy are not included in the copy of the software. Choice C is incorrect, as an IS auditor will have to gain this assurance separately. Choice D is incorrect, because any changes made between the time the control copy was acquired and the source code comparison is made will not be detected.

NEW QUESTION 296

- (Topic 2)

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

- A. confirm that the auditors did not overlook any important issue
- B. gain agreement on the finding
- C. receive feedback on the adequacy of the audit procedure
- D. test the structure of the final presentatio

Answer: B

Explanation:

The primary purpose for meeting with auditees prior to formally closing a review is to gain agreement on the findings. The other choices, though related to the formal closure of an audit, are of secondary importance.

NEW QUESTION 301

- (Topic 2)

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- A. Test data run
- B. Code review
- C. Automated code comparison
- D. Review of code migration procedures

Answer: C

Explanation:

An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure. Test data runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unexercised portions of a program. Code review is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

NEW QUESTION 305

- (Topic 2)

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

- A. include the statement of management in the audit report
- B. identify whether such software is, indeed, being used by the organization
- C. reconfirm with management the usage of the software
- D. discuss the issue with senior management since reporting this could have a negative impact on the organization

Answer: B

Explanation:

When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

NEW QUESTION 309

- (Topic 2)

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

- A. audit trail of the versioning of the work paper
- B. approval of the audit phase
- C. access rights to the work paper
- D. confidentiality of the work paper

Answer: D

Explanation:

Encryption provides confidentiality for the electronic work papers. Audit trails, audit phase approvals and access to the work papers do not, of themselves, affect the confidentiality but are part of the reason for requiring encryption.

NEW QUESTION 311

- (Topic 2)

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

- A. comply with regulatory requirement
- B. provide a basis for drawing reasonable conclusion
- C. ensure complete audit coverage
- D. perform the audit according to the defined scope

Answer: B

Explanation:

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

NEW QUESTION 314

- (Topic 2)

Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new enterprise resource planning (ERP) implementation?

- A. Reviewing a report of security rights in the system
- B. Reviewing the complexities of authorization objects
- C. Building a program to identify conflicts in authorization
- D. Examining recent access rights violation cases

Answer: C

Explanation:

Since the objective is to identify violations in segregation of duties, it is necessary to define the logic that will identify conflicts in authorization. A program could be developed to identify these conflicts. A report of security rights in the enterprise resource planning (ERP) system would be voluminous and time consuming to review; therefore, this technique is not as effective as building a program. As complexities increase, it becomes more difficult to verify the effectiveness of the systems and complexity is not, in itself, a link to segregation of duties. It is good practice to review recent access rights violation cases; however, it may require a significant amount of time to truly identify which violations actually resulted from an inappropriate segregation of duties.

NEW QUESTION 318

- (Topic 2)

Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

- A. System log analysis
- B. Compliance testing
- C. Forensic analysis
- D. Analytical review

Answer: B

Explanation:

Determining that only authorized modifications are made to production programs would require the change management process be reviewed to evaluate the existence of a trail of documentary evidence. Compliance testing would help to verify that the change management process has been applied consistently. It is unlikely that the system log analysis would provide information about the modification of programs. Forensic analysis is a specialized technique for criminal investigation. An analytical review assesses the general control environment of an organization.

NEW QUESTION 322

- (Topic 2)

An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

- A. decline the assignment
- B. inform management of the possible conflict of interest after completing the audit assignment
- C. inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment
- D. communicate the possibility of conflict of interest to management prior to starting the assignment

Answer: D

Explanation:

Communicating the possibility of a conflict of interest to management prior to starting the assignment is the correct answer. A possible conflict of interest, likely to affect the auditor's independence, should be brought to the attention of management prior to starting the assignment. Declining the assignment is not the correct answer because the assignment could be accepted after obtaining management approval. Informing management of the possible conflict of interest after completion of the audit assignment is not correct because approval should be obtained prior to commencement and not after the completion of the assignment. Informing the business continuity planning (BCP) team of the possible conflict of interest prior to starting of the assignment is not the correct answer since the BCP team would not have the authority to decide on this issue.

NEW QUESTION 327

- (Topic 2)

The success of control self-assessment (CSA) highly depends on:

- A. having line managers assume a portion of the responsibility for control monitoring
- B. assigning staff managers the responsibility for building, but not monitoring, control
- C. the implementation of a stringent control policy and rule-driven control
- D. the implementation of supervision and the monitoring of controls of assigned duties

Answer: A

Explanation:

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a control self-assessment (CSA) program depends on the degree to which line managers assume responsibility for controls. Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

NEW QUESTION 332

- (Topic 3)

Which of the following is a function of an IS steering committee?

- A. Monitoring vendor-controlled change control and testing
- B. Ensuring a separation of duties within the information's processing environment
- C. Approving and monitoring major projects, the status of IS plans and budgets
- D. Liaising between the IS department and the end users

Answer: C

Explanation:

The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

NEW QUESTION 334

- (Topic 3)

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- A. business plan
- B. audit plan
- C. security plan
- D. investment plan

Answer: A

Explanation:

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, while the security plan should be at a corporate level.

NEW QUESTION 338

- (Topic 3)

IT governance is PRIMARILY the responsibility of the:

- A. chief executive office
- B. board of director
- C. IT steering committee
- D. audit committee

Answer: B

Explanation:

IT governance is primarily the responsibility of the executives and shareholders (as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

NEW QUESTION 341

- (Topic 3)

As an outcome of information security governance, strategic alignment provides:

- A. security requirements driven by enterprise requirement
- B. baseline security following best practice
- C. institutionalized and commoditized solution
- D. an understanding of risk exposure

Answer: A

Explanation:

Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

NEW QUESTION 344

- (Topic 3)

Effective IT governance requires organizational structures and processes to ensure that:

- A. the organization's strategies and objectives extend the IT strategy
- B. the business strategy is derived from an IT strategy
- C. IT governance is separate and distinct from the overall governance
- D. the IT strategy extends the organization's strategies and objectives

Answer: D

Explanation:

Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

NEW QUESTION 347

- (Topic 3)

Which of the following is the MOST important element for the successful implementation of IT governance?

- A. Implementing an IT scorecard
- B. Identifying organizational strategies
- C. Performing a risk assessment
- D. Creating a formal security policy

Answer: B

Explanation:

The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies, the remaining choices—even if implemented—would be ineffective.

NEW QUESTION 349

- (Topic 3)

When implementing an IT governance framework in an organization the MOST important objective is:

- A. IT alignment with the business
- B. accountability
- C. value realization with IT
- D. enhancing the return on IT investment

Answer: A

Explanation:

The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business (choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

NEW QUESTION 354

- (Topic 3)

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- A. Repeatable but Intuitive
- B. Defined
- C. Managed and Measurable
- D. Optimized

Answer: B

Explanation:

Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

NEW QUESTION 357

- (Topic 3)

Responsibility for the governance of IT should rest with the:

- A. IT strategy committee
- B. chief information officer (CIO).
- C. audit committee
- D. board of director

Answer: D

Explanation:

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the chief information officer (CIO) and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

NEW QUESTION 360

- (Topic 3)

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- A. User acceptance testing (UAT) occur for all reports before release into production
- B. Organizational data governance practices be put in place
- C. Standard software tools be used for report development
- D. Management sign-off on requirements for new reports

Answer: B

Explanation:

This choice directly addresses the problem. An organizationwide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

NEW QUESTION 364

- (Topic 3)

Which of the following would BEST provide assurance of the integrity of new staff?

- A. Background screening
- B. References
- C. Bonding
- D. Qualifications listed on a resume

Answer: A

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

NEW QUESTION 365

- (Topic 3)

When an employee is terminated from service, the MOST important action is to:

- A. hand over all of the employee's files to another designated employe
- B. complete a backup of the employee's wor
- C. notify other employees of the terminatio
- D. disable the employee's logical acces

Answer: D

Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

NEW QUESTION 368

- (Topic 3)

Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

- A. ensure the employee maintains a good quality of life, which will lead to greater productivit
- B. reduce the opportunity for an employee to commit an improper or illegal ac
- C. provide proper cross-training for another employe
- D. eliminate the potential disruption caused when an employee takes vacation one day at a tim

Answer: B

Explanation:

Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

NEW QUESTION 372

- (Topic 3)

A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

- A. length of service, since this will help ensure technical competenc
- B. age, as training in audit techniques may be impractica
- C. IS knowledge, since this will bring enhanced credibility to the audit functio
- D. ability, as an IS auditor, to be independent of existing IS relationship

Answer: D

Explanation:

Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. The length of service will not ensure technical competency. Evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

NEW QUESTION 375

- (Topic 3)

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

- A. Deleting database activity logs
- B. Implementing database optimization tools
- C. Monitoring database usage
- D. Defining backup and recovery procedures

Answer: A

Explanation:

Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

NEW QUESTION 377

- (Topic 3)

Which of the following is normally a responsibility of the chief security officer (CSO)?

- A. Periodically reviewing and evaluating the security policy
- B. Executing user application and software testing and evaluation
- C. Granting and revoking user access to IT resources
- D. Approving access to data and applications

Answer: A

Explanation:

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

NEW QUESTION 379

- (Topic 3)

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

- A. there is an integration of IS and business staffs within project
- B. there is a clear definition of the IS mission and vision
- C. a strategic information technology planning methodology is in place
- D. the plan correlates business objectives to IS goals and objectives

Answer: A

Explanation:

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

NEW QUESTION 384

- (Topic 3)

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- A. Allocating resources
- B. Keeping current with technology advances
- C. Conducting control self-assessment
- D. Evaluating hardware needs

Answer: A

Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

NEW QUESTION 387

- (Topic 3)

Which of the following goals would you expect to find in an organization's strategic plan?

- A. Test a new accounting package
- B. Perform an evaluation of information technology need
- C. Implement a new project planning system within the next 12 months
- D. Become the supplier of choice for the product offered

Answer: D

Explanation:

Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

NEW QUESTION 389

- (Topic 3)

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

- A. has been approved by line management
- B. does not vary from the IS department's preliminary budget
- C. complies with procurement procedure
- D. supports the business objectives of the organization

Answer: D

Explanation:

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrect since line management prepared the plans.

NEW QUESTION 390

- (Topic 3)

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- A. incorporates state of the art technolog
- B. addresses the required operational control
- C. articulates the IT mission and visio
- D. specifies project management practice

Answer: C

Explanation:

The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

NEW QUESTION 392

- (Topic 3)

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- A. are developed for the organization as a whol
- B. are more likely to be derived as a result of a risk assessmen
- C. will not conflict with overall corporate polic
- D. ensure consistency across the organizatio

Answer: B

Explanation:

A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency across the organization.

NEW QUESTION 396

- (Topic 3)

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- A. User management coordination does not exis
- B. Specific user accountability cannot be establishe
- C. Unauthorized users may have access to originate, modify or delete dat
- D. Audit recommendations may not be implemente

Answer: C

Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

NEW QUESTION 397

- (Topic 3)

The rate of change in technology increases the importance of:

- A. outsourcing the IS functio
- B. implementing and enforcing good processe
- C. hiring personnel willing to make a career within the organizatio
- D. meeting user requirement

Answer: B

Explanation:

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

NEW QUESTION 402

- (Topic 3)

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- A. Response
- B. Correction
- C. Detection
- D. Monitoring

Answer: A

Explanation:

A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

NEW QUESTION 407

- (Topic 3)

Which of the following is the initial step in creating a firewall policy?

- A. A cost-benefit analysis of methods for securing the applications
- B. Identification of network applications to be externally accessed
- C. Identification of vulnerabilities associated with network applications to be externally accessed
- D. Creation of an applications traffic matrix showing protection methods

Answer: B

Explanation:

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

NEW QUESTION 410

- (Topic 3)

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

- A. recover
- B. retentio
- C. rebuildin
- D. reus

Answer: B

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic 'paper*' makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

NEW QUESTION 413

- (Topic 3)

A top-down approach to the development of operational policies will help ensure:

- A. that they are consistent across the organizatio
- B. that they are implemented as a part of risk assessmen
- C. compliance with all policie
- D. that they are reviewed periodicall

Answer: A

Explanation:

Deriving lower level policies from corporate policies (a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

NEW QUESTION 415

- (Topic 3)

Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

- A. Time zone differences could impede communications between IT team
- B. Telecommunications cost could be much higher in the first yea
- C. Privacy laws could prevent cross-border flow of informatio
- D. Software development may require more detailed specification

Answer: C

Explanation:

Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

NEW QUESTION 419

- (Topic 3)

A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

- A. Issues of privacy
- B. Wavelength can be absorbed by the human body
- C. RFID tags may not be removable
- D. RFID eliminates line-of-sight reading

Answer: A

Explanation:

The purchaser of an item will not necessarily be aware of the presence of the tag. If a tagged item is paid for by credit card, it would be possible to tie the unique ID of that item to the identity of the purchaser. Privacy violations are a significant concern because RFID can carry unique identifier numbers. If desired it would be possible for a firm to track individuals who purchase an item containing an RFID. Choices B and C are concerns of less importance. Choice D is not a concern.

NEW QUESTION 423

- (Topic 3)

The PRIMARY objective of implementing corporate governance by an organization's management is to:

- A. provide strategic direction
- B. control business operation
- C. align IT with business
- D. implement best practice

Answer: A

Explanation:

Corporate governance is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Hence, the primary objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

NEW QUESTION 426

- (Topic 3)

A benefit of open system architecture is that it:

- A. facilitates interoperability
- B. facilitates the integration of proprietary components
- C. will be a basis for volume discounts from equipment vendors
- D. allows for the achievement of more economies of scale for equipment

Answer: A

Explanation:

Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

NEW QUESTION 431

- (Topic 3)

After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- A. Project management and progress reporting is combined in a project management office which is driven by external consultants
- B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach
- C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy system
- D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs

Answer: B

Explanation:

The efforts should be consolidated to ensure alignment with the overall strategy of the postmerger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In postmerger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralize dependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. It is a good idea to first get familiar with the old systems, to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs as organizations and processes change to leverage the intended synergy effects of the merger.

NEW QUESTION 435

- (Topic 3)

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- A. Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan
- B. Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract

- C. No, because the backup to be provided should be specified adequately in the contract
- D. No, because the service bureau's business continuity plan is proprietary information

Answer: A

Explanation:

The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

NEW QUESTION 436

- (Topic 3)

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- A. O/S and hardware refresh frequencies
- B. Gain-sharing performance bonuses
- C. Penalties for noncompliance
- D. Charges tied to variable cost metrics

Answer: B

Explanation:

Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

NEW QUESTION 441

- (Topic 3)

When an organization is outsourcing their information security function, which of the following should be kept in the organization?

- A. Accountability for the corporate security policy
- B. Defining the corporate security policy
- C. Implementing the corporate security policy
- D. Defining security procedures and guidelines

Answer: A

Explanation:

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

NEW QUESTION 446

- (Topic 3)

With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

- A. Outsourced activities are core and provide a differentiated advantage to the organization
- B. Periodic renegotiation is specified in the outsourcing contract
- C. The outsourcing contract fails to cover every action required by the arrangement
- D. Similar activities are outsourced to more than one vendor

Answer: A

Explanation:

An organization's core activities generally should not be outsourced, because they are what the organization does best; an IS auditor observing that should be concerned. An IS auditor should not be concerned about the other conditions because specification of periodic renegotiation in the outsourcing contract is a best practice. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved, while multisourcing is an acceptable way to reduce risk.

NEW QUESTION 447

- (Topic 3)

Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

- A. Security incident summaries
- B. Vendor best practices
- C. CERT coordination center
- D. Significant contracts

Answer: D

Explanation:

Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets. Vendor best practices provides a basis for evaluating how competitive an enterprise is, while security incident summaries are a source for assessing the vulnerabilities associated with the IT infrastructure. CERT (www.cert.org) is an information source for assessing vulnerabilities within the IT infrastructure.

NEW QUESTION 452

- (Topic 3)

The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

- A. destruction polic
- B. security polic
- C. archive polic
- D. audit polic

Answer: C

Explanation:

With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

NEW QUESTION 453

- (Topic 3)

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- A. Report the risks to the CIO and CEO immediately
- B. Examine e-business application in development
- C. Identify threats and likelihood of occurrence
- D. Check the budget available for risk management

Answer: C

Explanation:

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

NEW QUESTION 455

- (Topic 3)

A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

- A. compute the amortization of the related asset
- B. calculate a return on investment (ROI).
- C. apply a qualitative approac
- D. spend the time needed to define exactly the loss amoun

Answer: C

Explanation:

The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor {e.g., one is a very low impact to thebusiness and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

NEW QUESTION 460

- (Topic 3)

Assessing IT risks is BEST achieved by:

- A. evaluating threats associated with existing IT assets and IT project
- B. using the firm's past actual loss experience to determine current exposur
- C. reviewing published loss statistics from comparable organization
- D. reviewing IT control weaknesses identified in audit report

Answer: A

Explanation:

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to beassessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

NEW QUESTION 461

- (Topic 3)

A poor choice of passwords and transmission over unprotected communications lines are examples of:

- A. vulnerabilitie
- B. threat
- C. probabilitie
- D. impact

Answer: A

Explanation:

Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat, while impacts represent the outcome or result of a threat exploiting a vulnerability.

NEW QUESTION 464

- (Topic 3)

An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

- A. address all of the network risk
- B. be tracked over time against the IT strategic pla
- C. take into account the entire IT environmen
- D. result in the identification of vulnerability tolerance

Answer: C

Explanation:

When assessing IT security risk, it is important to take into account the entire IT environment. Measures of security risk should focus on those areas with the highest criticality so as to achieve maximum risk reduction at the lowest possible cost. IT strategic plans are not granular enough to provide appropriate measures. Objective metrics must be tracked over time against measurable goals, thus the management of risk is enhanced by comparing today's results against last week, last month, last quarter. Risk measures will profile assets on a network to objectively measure vulnerability risk. They do not identify tolerances.

NEW QUESTION 468

- (Topic 3)

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

- A. performance measuremen
- B. strategic alignmen
- C. value deliver
- D. resource managemen

Answer: A

Explanation:

Performance measurement includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how they deliver it (process capability and performance). Strategic alignment primarily focuses on ensuring linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle. Resource management is about the optimal investment in and proper management of critical IT resources. Transparency is primarily achieved through performance measurement as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.

NEW QUESTION 473

- (Topic 3)

Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

- A. Process maturity
- B. Performance indicators
- C. Business risk
- D. Assurance reports

Answer: C

Explanation:

Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

NEW QUESTION 474

- (Topic 3)

Before implementing an IT balanced scorecard, an organization must:

- A. deliver effective and efficient service
- B. define key performance indicator
- C. provide business value to IT project
- D. control IT expense

Answer: B

Explanation:

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

NEW QUESTION 477

- (Topic 3)

Which of the following is the PRIMARY objective of an IT performance measurement process?

- A. Minimize errors
- B. Gather performance data
- C. Establish performance baselines
- D. Optimize performance

Answer: D

Explanation:

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of IT measurement process and would be used to evaluate the performance against previously established performance baselines.

NEW QUESTION 480

- (Topic 4)

When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

- A. a clear business case has been approved by management
- B. corporate security standards will be met
- C. users will be involved in the implementation plan
- D. the new system will meet all required user functionality

Answer: A

Explanation:

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as is meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be an IS auditor's first concern.

NEW QUESTION 483

- (Topic 4)

Documentation of a business case used in an IT development project should be retained until:

- A. the end of the system's life cycle
- B. the project is approved
- C. user acceptance of the system
- D. the system is in production

Answer: A

Explanation:

A business case can and should be used throughout the life cycle of the product. It serves as an anchor for new (management) personnel, helps to maintain focus and provides valuable information on estimates vs. actuals. Questions like, 'why do we do that,' 'what was the original intent' and 'how did we perform against the plan' can be answered, and lessons for developing future business cases can be learned. During the development phase of a project one should always validate the business case, as it is a good management instrument. After finishing a project and entering production, the business case and all the completed research are valuable sources of information that should be kept for further reference.

NEW QUESTION 487

- (Topic 4)

Which of the following risks could result from inadequate software baselining?

- A. Scope creep
- B. Sign-off delays
- C. Software integrity violations
- D. inadequate controls

Answer: A

Explanation:

A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a business cost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. Choices B, C and D may not always result, but choice A is inevitable.

NEW QUESTION 488

- (Topic 4)

The reason for establishing a stop or freezing point on the design of a new system is to:

- A. prevent further changes to a project in process
- B. indicate the point at which the design is to be complete
- C. require that changes after that point be evaluated for cost-effectiveness
- D. provide the project management team with more control over the project design

Answer: C

Explanation:

Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost-benefits and the payback period.

NEW QUESTION 489

- (Topic 4)

Change control for business application systems being developed using prototyping could be complicated by the:

- A. iterative nature of prototyping
- B. rapid pace of modifications in requirements and design
- C. emphasis on reports and screens
- D. lack of integrated tool

Answer: B

Explanation:

Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

NEW QUESTION 490

- (Topic 4)

When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

- A. The project budget
- B. The critical path for the project
- C. The length of the remaining tasks
- D. The personnel assigned to other tasks

Answer: B

Explanation:

Since adding resources may change the route of the critical path, the critical path must be reevaluated to ensure that additional resources will in fact shorten the project duration. Given that there may be slack time available on some of the other tasks not on the critical path, factors such as the project budget, the length of other tasks and the personnel assigned to them may or may not be affected.

NEW QUESTION 494

- (Topic 4)

To minimize the cost of a software project, quality management techniques should be applied:

- A. as close to their writing (i.e., point of origination) as possible
- B. primarily at project start-up to ensure that the project is established in accordance with organizational governance standards
- C. continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate
- D. mainly at project close-down to capture lessons learned that can be applied to future projects

Answer: C

Explanation:

While it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is that the earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

NEW QUESTION 495

- (Topic 4)

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

- A. whose sum of activity time is the shortest
- B. that have zero slack time
- C. that give the longest possible completion time
- D. whose sum of slack time is the shortest

Answer: B

Explanation:

A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities on the critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

NEW QUESTION 496

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISA Exam with Our Prep Materials Via below:

<https://www.certleader.com/CISA-dumps.html>